

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-184314
(P2001-184314A)

(43) 公開日 平成13年7月6日 (2001.7.6)

(51) IntCl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 1 7
12/00	5 4 5	12/00	5 4 5 M 5 B 0 4 9
12/14	3 2 0	12/14	3 2 0 B 5 B 0 8 2
13/00	3 5 4	13/00	3 5 4 Z 5 B 0 8 5
17/60	Z E C	15/21	Z E C Z 5 B 0 8 9

審査請求 未請求 請求項の数12 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平11-370556

(22) 出願日 平成11年12月27日 (1999. 12. 27)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 永井 規浩

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100092152

弁理士 服部 毅蔵

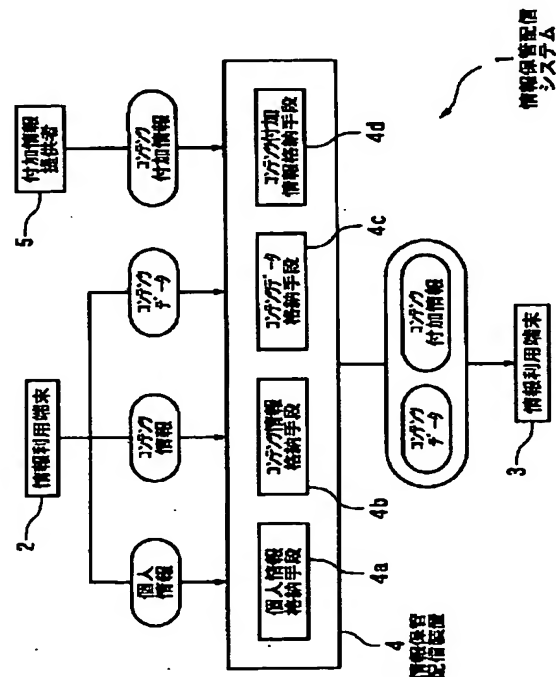
最終頁に続く

(54) 【発明の名称】 情報利用端末、情報保管配信装置、情報保管配信システム及び記録媒体

(57) 【要約】

【課題】 使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行う。

【解決手段】 利用者が使用権を取得したコンテンツを、情報利用端末2を用いて情報保管配信装置4に送信し、情報保管配信装置4は、そのコンテンツを保管し、利用者が情報保管配信装置4に格納されたコンテンツの利用を希望する場合、利用者は情報利用端末3を用いて情報保管配信装置4に格納されたコンテンツの配信を要求し、情報保管配信装置4は、要求されたコンテンツをコンテンツ付加情報とともに情報利用端末3に配信する。



1

【特許請求の範囲】

【請求項 1】 コンテンツデータの利用を行う情報利用
端末において、

前記コンテンツデータの保管及び配信を行う情報保管配
信装置に送信する前記コンテンツデータの選択を行う送
信コンテンツ選択手段と、

前記送信コンテンツ選択手段によって選択された前記コ
ンテンツデータをコンテンツ鍵によって暗号化するコン
テンツ鍵暗号化手段と、

端末秘密鍵によって前記コンテンツ鍵を暗号化する端末
秘密鍵暗号化手段と、

前記情報保管配信装置との認証処理を行い、前記情報保
管配信装置との共有鍵であるセッション鍵を生成する認
証手段と、

前記端末秘密鍵暗号化手段によって暗号化された前記コ
ンテンツ鍵を、前記セッション鍵により暗号化するセッ
ション鍵暗号化手段と、

前記コンテンツ鍵暗号化手段によって暗号化された前記
コンテンツデータ、前記セッション鍵暗号化手段によっ
て暗号化された前記コンテンツ鍵、及び前記コンテンツ
データの内容を示すコンテンツ情報を前記情報保管配信
装置に送信する情報送信手段と、
を有することを特徴とする情報利用端末。

【請求項 2】 配信を希望するコンテンツの選択を行う
配信コンテンツ選択手段と、

前記配信コンテンツ選択手段による選択に応じて抽出さ
れ、前記コンテンツ鍵によって暗号化された前記コンテ
ンツデータ、前記端末秘密鍵によって暗号化され、さら
に前記セッション鍵により暗号化された前記コンテンツ
鍵、及び前記セッション鍵によって暗号化されたコンテ
ンツ付加情報を受信する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受
信された前記コンテンツ鍵及び前記コンテンツ付加情報
を復号するセッション鍵復号手段と、

前記端末秘密鍵により、前記セッション鍵によって復号
された前記コンテンツ鍵を復号する端末秘密鍵復号手段
と、

前記端末秘密鍵復号手段によって復号された前記コンテ
ンツ鍵により、前記コンテンツデータを復号するコンテ
ンツ鍵復号手段と、

をさらに有することを特徴とする請求項 1 記載の情報利
用端末。

【請求項 3】 前記セッション鍵により暗号化され、前
記情報保管配信装置から送信されたコンテンツリストを
受信するコンテンツリスト受信手段と、

前記コンテンツリスト受信手段によって受信された前記
コンテンツリストを前記セッション鍵により復号するコ
ンテンツリスト復号手段と、

をさらに有することを特徴とする請求項 2 記載の情報利
用端末。

2

【請求項 4】 コンテンツデータの利用を行う情報利用
端末において、

前記コンテンツデータの保管及び配信を行う情報保管配
信装置との認証処理を行い、前記情報保管配信装置との
共有鍵であるセッション鍵を生成する認証手段と、

配信を希望するコンテンツの選択を行う配信コンテンツ
選択手段と、

前記配信コンテンツ選択手段による選択に応じて抽出さ
れ、コンテンツ鍵によって暗号化された前記コンテンツ
データ、端末秘密鍵によって暗号化され、さらに前記セ
ッション鍵により暗号化された前記コンテンツ鍵、及び

前記セッション鍵によって暗号化されたコンテンツ付加
情報を受信する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受
信された前記コンテンツ鍵及び前記コンテンツ付加情報
を復号するセッション鍵復号手段と、

前記端末秘密鍵により、前記セッション鍵によって復号
された前記コンテンツ鍵を復号する端末秘密鍵復号手段
と、

前記端末秘密鍵復号手段によって復号された前記コンテ
ンツ鍵により、前記コンテンツデータを復号するコンテ
ンツ鍵復号手段と、

を有することを特徴とする情報利用端末。

【請求項 5】 前記セッション鍵により暗号化され、前
記情報保管配信装置から送信されたコンテンツリストを
受信するコンテンツリスト受信手段と、

前記コンテンツリスト受信手段によって受信された前記
コンテンツリストを前記セッション鍵により復号するコ
ンテンツリスト復号手段と、

をさらに有することを特徴とする請求項 4 記載の情報利
用端末。

【請求項 6】 コンテンツデータの保管及び配信を行う
情報保管配信装置において、

前記コンテンツデータの利用を行う情報利用端末との認
証処理を行い、前記情報利用端末との共有鍵であるセッ
ション鍵を生成する認証手段と、

コンテンツ鍵によって暗号化された前記コンテンツデー
タ、端末秘密鍵によって暗号化され、さらに前記セッ
ション鍵によって暗号化された前記コンテンツ鍵、及び前
記コンテンツデータの内容を示すコンテンツ情報を受信

する情報受信手段と、

前記セッション鍵により、前記情報受信手段によって受
信された前記コンテンツ鍵を復号するセッション鍵復号
手段と、

センタ秘密鍵によって、前記セッション鍵復号手段によ
り復号された前記コンテンツ鍵を暗号化するセンタ秘密
鍵暗号化手段と、

前記情報受信手段によって受信された前記コンテンツデ
ータ、及び前記センタ秘密鍵暗号化手段によって暗号化
された前記コンテンツ鍵を格納するコンテンツデータ格

3

納手段と、
 前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、
 利用者の個人情報を格納する個人情報格納手段と、
 付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、
 前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、
 前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、
 コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、
 前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、
 前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段と、
 を有することを特徴とする情報保管配信装置。

【請求項7】 前記コンテンツ付加情報抽出手段は、前記個人情報及び前記コンテンツ情報に基づいて、前記コンテンツ付加情報の抽出を行うことを特徴とする請求項6記載の情報保管配信装置。

【請求項8】 前記コンテンツデータ格納手段に格納された前記コンテンツデータのリストであるコンテンツリストを作成するコンテンツリスト作成手段と、
 前記コンテンツリスト作成手段によって作成された前記コンテンツリストを前記セッション鍵により暗号化するコンテンツリスト暗号化手段と、
 前記コンテンツリスト暗号化手段によって暗号化された前記コンテンツリストを前記情報利用端末に送信するコンテンツリスト送信手段と、
 をさらに有することを特徴とする請求項6記載の情報保管配信装置。

【請求項9】 コンテンツデータの保管及び配信を行う情報保管配信システムにおいて、
 送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、認証処理を行い、共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コン

4

テンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する情報送信手段とを有する情報利用端末と、

配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、前記コンテンツ鍵によって暗号化された前記コンテンツデータ、前記端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、
 前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有する情報利用端末と、

前記情報利用端末との認証処理を行い、前記セッション鍵を生成する認証手段と、前記情報利用端末から送信された前記コンテンツデータ、前記コンテンツ鍵、及び前記コンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、
 センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータを、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信

する情報配信手段とを有する情報保管配信装置と、
を有することを特徴とする情報保管配信システム。

【請求項 10】 送信するコンテンツデータの選択を行
い、

選択された前記コンテンツデータをコンテンツ鍵によっ
て暗号化し、

端末秘密鍵によって前記コンテンツ鍵を暗号化し、

認証処理を行い、共有鍵であるセッション鍵を生成し、
暗号化された前記コンテンツ鍵を前記セッション鍵により
暗号化し、

暗号化された前記コンテンツデータ、前記コンテンツ
鍵、及び前記コンテンツデータの内容を示すコンテンツ
情報を送信する機能をコンピュータに行わせるプログラ
ムを格納する記録媒体。

【請求項 11】 認証処理を行い、共有鍵であるセッシ
ョン鍵を生成し、

配信を希望するコンテンツの選択を行い、

利用者の選択に応じて抽出され、コンテンツ鍵によっ
て暗号化されたコンテンツデータ、端末秘密鍵によっ
て暗号化され、さらに前記セッション鍵により暗号化され
た前記コンテンツ鍵、及び前記セッション鍵によっ
て暗号化されたコンテンツ付加情報を受信し、

受信された前記コンテンツ鍵及び前記コンテンツ付加情
報を前記セッション鍵により復号し、

前記セッション鍵によって復号された前記コンテンツ鍵
を前記端末秘密鍵により復号し、

復号された前記コンテンツ鍵により、前記コンテンツデ
ータを復号する機能をコンピュータに行わせるプログラ
ムを格納する記録媒体。

【請求項 12】 認証処理を行い、共有鍵であるセッシ
ョン鍵を生成し、

コンテンツ鍵によって暗号化された前記コンテンツデー
タ、端末秘密鍵によって暗号化され、さらに前記セッシ
ョン鍵によって暗号化された前記コンテンツ鍵、及び前
記コンテンツデータの内容を示すコンテンツ情報を受信
し、

前記セッション鍵により、前記情報受信手段によって受
信された前記コンテンツ鍵を復号し、

センタ秘密鍵によって、前記セッション鍵復号手段によ
り復号された前記コンテンツ鍵を暗号化し、

受信した前記コンテンツデータ、及び暗号化された前記
コンテンツ鍵を格納し、

受信した前記コンテンツ情報を格納し、

利用者の個人情報を格納し、

付加情報提供者が提供するコンテンツ付加情報を格納
し、

各利用者に応じた前記コンテンツ付加情報を抽出し、

利用者に選択された前記コンテンツデータ及び前記コン
テンツ鍵を抽出し、

抽出された前記コンテンツ鍵を前記センタ秘密鍵により

復号し、

復号された前記コンテンツ鍵、及び抽出された前記コン
テンツ付加情報を前記セッション鍵によって暗号化し、
抽出された前記コンテンツデータ、及び暗号化された前
記コンテンツ鍵及び前記コンテンツ付加情報を配信する
機能をコンピュータに行わせるプログラムを格納した記
録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツデー
タの利用を行う情報利用端末、コンテンツデータの保管及
び配信を行う情報保管配信装置、情報保管配信システ
ム、及びそれらの機能をコンピュータに行わせるプログラ
ムを格納した記録媒体に関し、特に、通信ネットワー
クを利用した情報利用端末、情報保管配信装置、情報保
管配信システム、及びそれらの機能をコンピュータに行
わせるプログラムを格納した記録媒体に関する。

【0002】

【従来の技術】従来、音楽、映像等のコンテンツの使用
権取得は、CD、DVD等のコンテンツデータが格納さ
れた記録媒体を購入するか、インターネット等の電子通
信回線を通じ、コンテンツデータをダウンロードするこ
とによって行われてきた。電子通信回線を通じてダウン
ロードしたコンテンツデータは、その電子通信回線に接
続されたコンピュータ等有するハードディスク等の記
録装置、或いはメモリースティック、フロッピーディス
ク、MD等の記録媒体に格納され、利用者は、それらに
格納されたコンテンツを再生することにより、取得した
コンテンツの利用を行うことができる。

【0003】

【発明が解決しようとする課題】しかし、ダウンロード
したコンテンツデータを記録装置に格納する方法では、
記録装置が有する記憶容量を上限として、保有できるコ
ンテンツが制限されてしまうという問題点がある。

【0004】また、CD等の記録媒体を入手する方法、
及びダウンロードしたコンテンツデータを記録媒体に格
納する方法では、利用者は、コンテンツデータを格納し
た記録媒体を別途保管しておかなければならないため、
管理上の利便性に欠け、コンテンツ再生時におけるコン
テンツの選択が困難であるという問題点がある。

【0005】さらに、コンテンツデータを格納した記録
媒体を用いる場合、この記録媒体を所持していない場合
においては、コンテンツの再生を行うことができないと
いう問題点もある。

【0006】また、コンテンツデータを格納した記録媒
体を用いる場合、コンテンツを再生する情報利用装置に
はこの記録媒体の収納部及び駆動部が必要となり、情報
利用装置の小型化が図れないという問題点もある。

【0007】さらに、従来の方法では、取得したコンテ
ンツに関する最新情報等の入手は、利用者が別途に行わ

7

なければならないという問題点がある。本発明はこのような点に鑑みてなされたものであり、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、装置の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報利用端末を提供することを目的とする。

【0008】また、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報保管配信装置を提供することである。

【0009】さらに、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能な情報保管配信システムを提供することである。

【0010】また、本発明の他の目的は、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下であってもコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者へ利用者に適した各種情報の提供を可能とする機能をコンピュータに行わせるプログラムを格納した記録媒体を提供することである。

【0011】

【課題を解決するための手段】本発明では上記課題を解決するために、コンテンツデータの利用を行う情報利用端末において、前記コンテンツデータの保管及び配信を行う情報保管配信装置に送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、前記情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を前記情報保管配信装置に送信する情報送信手段とを有することを特徴とする情報利用端末が提供される。

8

【0012】ここで、送信コンテンツ選択手段は、情報保管配信装置に送信するコンテンツデータの選択を行い、コンテンツ鍵暗号化手段は、送信コンテンツ選択手段によって選択されたコンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵暗号化手段は、端末秘密鍵によってコンテンツ鍵を暗号化し、認証手段は、情報保管配信装置との認証処理を行い、情報保管配信装置との共有鍵であるセッション鍵を生成し、セッション鍵暗号化手段は、端末秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を、セッション鍵により暗号化し、情報送信手段は、コンテンツ鍵暗号化手段によって暗号化されたコンテンツデータ、セッション鍵暗号化手段によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を情報保管配信装置に送信する。

【0013】また、コンテンツデータの利用を行う情報利用端末において、前記コンテンツデータの保管及び配信を行う情報保管配信装置との認証処理を行い、前記情報保管配信装置との共有鍵であるセッション鍵を生成する認証手段と、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有することを特徴とする情報利用端末が提供される。

【0014】ここで、認証手段は、情報保管配信装置との認証処理を行い、情報保管配信装置との共有鍵であるセッション鍵を生成し、配信コンテンツ選択手段は、配信を希望するコンテンツの選択を行い、情報受信手段は、配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ鍵、及びセッション鍵によって暗号化されたコンテンツ付加情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵及びコンテンツ付加情報をセッション鍵により復号し、端末秘密鍵復号手段は、セッション鍵によって復号されたコンテンツ鍵を端末秘密鍵により復号し、コンテンツ鍵復号手段は、端末秘密鍵復号手段によって復号されたコンテンツ鍵によりコンテンツデータを

復号する。

【0015】さらに、コンテンツデータの保管及び配信を行う情報保管配信装置において、前記コンテンツデータの利用を行う情報利用端末との認証処理を行い、前記情報利用端末との共有鍵であるセッション鍵を生成する認証手段と、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段とを有することを特徴とする情報保管配信装置が提供される。

【0016】ここで、認証手段は、情報利用端末との認証処理を行い、情報利用端末との共有鍵であるセッション鍵を生成し、情報受信手段は、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵をセッション鍵により復号し、センタ秘密鍵暗号化手段は、セッション鍵復号手段によりコンテンツデータ格納手段は、情報受信手段によって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を

格納し、コンテンツ情報格納手段は、情報受信手段によって受信されたコンテンツ情報を格納し、個人情報格納手段は、利用者の個人情報を格納し、コンテンツ付加情報格納手段は、付加情報提供者が提供するコンテンツ付加情報を格納し、コンテンツ付加情報抽出手段は、コンテンツ付加情報格納手段から、各利用者に応じたコンテンツ付加情報を抽出し、コンテンツ抽出手段は、コンテンツデータ格納手段から、選択されたコンテンツデータ及びコンテンツ鍵を抽出し、センタ秘密鍵復号手段は、コンテンツ抽出手段によって抽出されたコンテンツ鍵をセンタ秘密鍵により復号し、セッション鍵暗号化手段は、センタ秘密鍵復号手段によって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段によって抽出されたコンテンツ付加情報をセッション鍵によって暗号化し、情報配信手段は、コンテンツ抽出手段により抽出されたコンテンツデータ、及びセッション鍵暗号化手段により暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末に配信する。

【0017】また、コンテンツデータの保管及び配信を行う情報保管配信システムにおいて、送信する前記コンテンツデータの選択を行う送信コンテンツ選択手段と、前記送信コンテンツ選択手段によって選択された前記コンテンツデータをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段と、端末秘密鍵によって前記コンテンツ鍵を暗号化する端末秘密鍵暗号化手段と、認証処理を行い、共有鍵であるセッション鍵を生成する認証手段と、前記端末秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化するセッション鍵暗号化手段と、前記コンテンツ鍵暗号化手段によって暗号化された前記コンテンツデータ、前記セッション鍵暗号化手段によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する情報送信手段とを有する情報利用端末と、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段と、前記配信コンテンツ選択手段による選択に応じて抽出され、前記コンテンツ鍵によって暗号化された前記コンテンツデータ、前記端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によって暗号化されたコンテンツ付加情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵及び前記コンテンツ付加情報を復号するセッション鍵復号手段と、前記端末秘密鍵により、前記セッション鍵によって復号された前記コンテンツ鍵を復号する端末秘密鍵復号手段と、前記端末秘密鍵復号手段によって復号された前記コンテンツ鍵により、前記コンテンツデータを復号するコンテンツ鍵復号手段とを有する情報利用端末と、前記情報利用端末との認証処理を行い、前記セッション鍵を生成する認証手段と、前記情報利用端末から送信された前記コンテン

11

ッデータ、前記コンテンツ鍵、及び前記コンテンツ情報を受信する情報受信手段と、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号するセッション鍵復号手段と、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段と、前記情報受信手段によって受信された前記コンテンツデータ、及び前記センタ秘密鍵暗号化手段によって暗号化された前記コンテンツ鍵を格納するコンテンツデータ格納手段と、前記情報受信手段によって受信された前記コンテンツ情報を格納するコンテンツ情報格納手段と、利用者の個人情報を格納する個人情報格納手段と、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段と、前記コンテンツ付加情報格納手段から、各利用者に応じた前記コンテンツ付加情報を抽出するコンテンツ付加情報抽出手段と、前記コンテンツデータ格納手段から、選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出するコンテンツ抽出手段と、コンテンツ抽出手段によって抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号するセンタ秘密鍵復号手段と、前記センタ秘密鍵復号手段によって復号された前記コンテンツ鍵、及び前記コンテンツ付加情報抽出手段によって抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化するセッション鍵暗号化手段と、前記コンテンツ抽出手段により抽出された前記コンテンツデータ、及び前記セッション鍵暗号化手段により暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を前記情報利用端末に配信する情報配信手段とを有する情報保管配信装置とを有することを特徴とする情報保管配信システムが提供される。

【0018】ここで、送信コンテンツ選択手段は、送信するコンテンツデータの選択を行い、コンテンツ鍵暗号化手段は、送信コンテンツ選択手段によって選択されたコンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵暗号化手段は、端末秘密鍵によってコンテンツ鍵を暗号化し、認証手段は、認証処理を行い、共有鍵であるセッション鍵を生成し、セッション鍵暗号化手段は、端末秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を、セッション鍵により暗号化し、情報送信手段は、コンテンツ鍵暗号化手段によって暗号化されたコンテンツデータ、セッション鍵暗号化手段によって暗号化されたコンテンツ鍵、及びコンテンツデータの内容を示すコンテンツ情報を送信し、配信コンテンツ選択手段は、配信を希望するコンテンツの選択を行い、情報受信手段は、配信コンテンツ選択手段による選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ鍵、及びセッション鍵によって暗号化されたコンテンツ付加情報を受信し、セッション鍵復号手段は、セッション鍵により、情

12

報受信手段によって受信されたコンテンツ鍵及びコンテンツ付加情報を復号し、端末秘密鍵復号手段は、端末秘密鍵により、セッション鍵によって復号されたコンテンツ鍵を復号し、コンテンツ鍵復号手段は、端末秘密鍵復号手段によって復号されたコンテンツ鍵により、コンテンツデータを復号し、認証手段は、情報利用端末との認証処理を行い、セッション鍵を生成し、情報受信手段は、情報利用端末から送信されたコンテンツデータ、コンテンツ鍵、及びコンテンツ情報を受信し、セッション鍵復号手段は、情報受信手段によって受信されたコンテンツ鍵をセッション鍵により復号し、センタ秘密鍵暗号化手段は、セッション鍵復号手段により復号されたコンテンツ鍵をセンタ秘密鍵により暗号化し、コンテンツデータ格納手段は、情報受信手段によって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段によって暗号化されたコンテンツ鍵を格納し、コンテンツ情報格納手段は、情報受信手段によって受信されたコンテンツ情報を格納し、個人情報格納手段は、利用者の個人情報を格納し、コンテンツ付加情報格納手段は、付加情報提供者が提供するコンテンツ付加情報を格納し、コンテンツ付加情報抽出手段は、コンテンツ付加情報格納手段から、各利用者に応じたコンテンツ付加情報を抽出し、コンテンツ抽出手段は、コンテンツデータ格納手段から、選択されたコンテンツデータ及びコンテンツ鍵を抽出し、センタ秘密鍵復号手段は、コンテンツ抽出手段によって抽出されたコンテンツ鍵をセンタ秘密鍵により復号し、セッション鍵暗号化手段は、センタ秘密鍵復号手段によって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段によって抽出されたコンテンツ付加情報をセッション鍵によって暗号化し、情報配信手段は、コンテンツ抽出手段により抽出されたコンテンツデータ、及びセッション鍵暗号化手段により暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末に配信する。

【0019】さらに、送信するコンテンツデータの選択を行い、選択された前記コンテンツデータをコンテンツ鍵によって暗号化し、端末秘密鍵によって前記コンテンツ鍵を暗号化し、認証処理を行い、共有鍵であるセッション鍵を生成し、暗号化された前記コンテンツ鍵を、前記セッション鍵により暗号化し、暗号化された前記コンテンツデータ、前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を送信する機能をコンピュータに行わせるプログラムを格納する記録媒体が提供される。

【0020】また、認証処理を行い、共有鍵であるセッション鍵を生成し、配信を希望するコンテンツの選択を行い、利用者の選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵により暗号化された前記コンテンツ鍵、及び前記セッション鍵によ

13

て暗号化されたコンテンツ付加情報を受信し、受信された前記コンテンツ鍵及び前記コンテンツ付加情報を前記セッション鍵により復号し、前記セッション鍵によって復号された前記コンテンツ鍵を前記端末秘密鍵により復号し、復号された前記コンテンツ鍵により、前記コンテンツデータを復号する機能をコンピュータに行わせるプログラムを格納する記録媒体が提供される。

【0021】さらに、認証処理を行い、共有鍵であるセッション鍵を生成し、コンテンツ鍵によって暗号化された前記コンテンツデータ、端末秘密鍵によって暗号化され、さらに前記セッション鍵によって暗号化された前記コンテンツ鍵、及び前記コンテンツデータの内容を示すコンテンツ情報を受信し、前記セッション鍵により、前記情報受信手段によって受信された前記コンテンツ鍵を復号し、センタ秘密鍵によって、前記セッション鍵復号手段により復号された前記コンテンツ鍵を暗号化し、受信した前記コンテンツデータ、及び暗号化された前記コンテンツ鍵を格納し、受信した前記コンテンツ情報を格納し、利用者の個人情報を格納し、付加情報提供者が提供するコンテンツ付加情報を格納し、各利用者に応じた前記コンテンツ付加情報を抽出し、利用者を選択された前記コンテンツデータ及び前記コンテンツ鍵を抽出し、抽出された前記コンテンツ鍵を前記センタ秘密鍵により復号し、復号された前記コンテンツ鍵、及び抽出された前記コンテンツ付加情報を前記セッション鍵によって暗号化し、抽出された前記コンテンツデータ、及び暗号化された前記コンテンツ鍵及び前記コンテンツ付加情報を配信する機能をコンピュータに行わせるプログラムを格納した記録媒体が提供される。

【0022】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は、本形態における情報保管配信システム1の概略構成を示した構成図である。

【0023】情報保管配信システム1は、コンテンツデータの利用を行う情報利用端末2、3、コンテンツデータの保管及び配信を行う情報保管配信装置4、及びコンテンツ付加情報の提供を行う付加情報提供者5によって構成されている。情報保管配信装置4は、利用者の個人情報を格納する個人情報格納手段4a、同じく情報利用端末2から送信されたコンテンツ情報を格納するコンテンツ情報格納手段4b、コンテンツデータを格納するコンテンツデータ格納手段4c、及び付加情報提供者5から提供された付加情報を格納するコンテンツ付加情報格納手段4dを有している。

【0024】ここで、個人情報とは、本システムの利用者の個人情報であり、利用者の氏名、性別、住所、端末ID、クレジットカード番号、利用者が配信を希望する情報、配信を希望しない情報等が含まれる。また、コンテンツデータとは、音楽、映像等のデータであり、利用者は、インターネットからのダウンロード、CD等の購

14

入によりそれらの使用権を取得する。コンテンツデータは、デジタルデータとして扱い得るデータであり、データ送信時等にはコンテンツ鍵を用いて暗号化される。コンテンツ情報とは、コンテンツジャンル等のコンテンツデータの内容を示したデータ、及び利用者が設定した情報により構成され、例えば、コンテンツデータが音楽コンテンツの場合、音楽のタイトル、演奏者名、コンテンツ制作団体名等の情報が含まれる。コンテンツ付加情報とは、付加情報提供者5が提供するコンテンツに付加することを希望する情報、例えば、音楽コンテンツに関するものであれば、新譜情報、新譜ダウンロード先、演奏家情報、及びダウンロードサイト等の広告情報等であり、テキストデータの他、画像データ、音声データ等も含まれる。

【0025】情報利用端末2は、本システムの利用者が使用権を取得したコンテンツを情報保管配信装置4に送信する装置であり、使用権を取得したコンテンツの保持を安全に行い、情報保管配信装置4とのコンテンツのやりとりを改竄、盗聴等の不正行為を防止しつつ行うことができる機能を有する。また、インターネットに接続する通信機能、及びWebページを表示する機能を有しており、これらにより、インターネットのダウンロードサイトからコンテンツの取得を行う。さらに、情報保管配信装置4へのコンテンツの送信処理を行うためのGUI (graphical user interface) ソフトウェアを有し、情報保管配信装置4が発行する本システム使用のための証明書を格納する記録装置を有している。

【0026】情報利用端末3は、情報保管配信装置4から配信されたコンテンツを受信し、その利用を行う装置であり、情報保管配信装置4と接続するための移動体通信等の通信手段を有し、受信したコンテンツを格納する記憶装置、及びコンテンツ情報を表示する表示部を有している。

【0027】情報保管配信装置4は、情報利用端末2から送信されたコンテンツ、及び付加情報提供者から送信されたコンテンツ付加情報を保管し、要求に応じて、保管されているコンテンツ及びコンテンツ付加情報を情報利用端末3に配信する装置である。

【0028】付加情報提供者5は、コンテンツ付加情報の提供者であり、コンテンツのダウンロードサイト、コンテンツ所有者、コンテンツ制作者、企業、個人提供者等が含まれる。

【0029】図2は、情報利用端末2の構成を示した構成図である。情報利用端末2は、使用権を取得したコンテンツデータを格納するコンテンツデータ格納手段2a、コンテンツデータ格納手段2aに格納されたコンテンツのコンテンツ情報を格納するコンテンツ情報格納手段2b、情報保管配信装置4に送信するコンテンツデータの選択を行う送信コンテンツ選択手段2c、送信コンテンツ選択手段2cによって選択されたコンテンツデー

15

タをコンテンツ鍵によって暗号化するコンテンツ鍵暗号化手段2 d、端末秘密鍵によってコンテンツ鍵を暗号化する端末秘密鍵暗号化手段2 e、情報保管配信装置4との認証処理を行い、情報保管配信装置4との共有鍵であるセッション鍵を生成する認証手段2 f、端末秘密鍵暗号化手段2 eによって暗号化されたコンテンツ鍵を、セッション鍵により暗号化するセッション鍵暗号化手段2 h、コンテンツ鍵暗号化手段2 dによって暗号化されたコンテンツデータ、セッション鍵暗号化手段2 hによって暗号化されたコンテンツ鍵、コンテンツ情報、及び個人情報情報を情報保管配信装置4に送信する情報送信手段2 iによって構成されている。

【0030】ここで、コンテンツ鍵とは、コンテンツデータを暗号化及び復号する際に用いる鍵であり、暗号化されたコンテンツデータとともに情報保管配信装置4に送信される。端末秘密鍵とは、情報保管配信装置4への送信時にコンテンツ鍵を暗号化する際に用いる秘密鍵であり、情報利用端末2が有する図示していないモジュールに保持される。セッション鍵とは、後述する認証によって生成される情報利用端末2、3と情報保管配信装置4との共有鍵であり、端末秘密鍵によって暗号化されたコンテンツ鍵等をさらに暗号化及び復号するために用いる鍵である。

【0031】図3は、情報利用端末3の構成を示した構成図である。情報利用端末3は、情報保管配信装置4との認証処理を行い、情報保管配信装置4との共有鍵であるセッション鍵を生成する認証手段3 a、セッション鍵により暗号化され、情報保管配信装置4から送信されたコンテンツリストを受信するコンテンツリスト受信手段3 b、コンテンツリスト受信手段3 bによって受信されたコンテンツリストをセッション鍵により復号するコンテンツリスト復号手段3 c、配信を希望するコンテンツの選択を行う配信コンテンツ選択手段3 d、配信コンテンツ選択手段3 dによる選択に応じて抽出され、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵により暗号化されたコンテンツ付加情報を受信する情報受信手段3 e、情報受信手段3 eによって受信されたコンテンツ鍵及びコンテンツ付加情報をセッション鍵により復号するセッション鍵復号手段3 f、端末秘密鍵により、セッション鍵によって復号されたコンテンツ鍵を復号する端末秘密鍵復号手段3 g、及び端末秘密鍵復号手段3 gによって復号されたコンテンツ鍵により、コンテンツデータを復号するコンテンツ鍵復号手段3 hによって構成されている。

【0032】ここで、コンテンツリストとは、情報保管配信装置4のコンテンツデータ格納手段4 cに格納されたコンテンツデータを示すリストであり、利用者はこのリストを参照し、配信を希望するコンテンツの選択を行

16

う。

【0033】図4は、情報保管配信装置4の構成を示した構成図である。情報保管配信装置4は、情報利用端末2、3との認証処理を行い、情報利用端末2、3との共有鍵であるセッション鍵を生成する認証手段4 e、コンテンツリストを作成するコンテンツリスト作成手段4 n、コンテンツデータ格納手段4 cに格納されたコンテンツデータのリストであるコンテンツリストを、セッション鍵により暗号化するコンテンツリスト暗号化手段4 o、コンテンツリスト暗号化手段4 oによって暗号化されたコンテンツリストを情報利用端末3に送信するコンテンツリスト送信手段4 p、コンテンツ鍵によって暗号化されたコンテンツデータ、端末秘密鍵によって暗号化され、さらにセッション鍵によって暗号化されたコンテンツ鍵、及びコンテンツ情報を受信する情報受信手段4 f、セッション鍵により、情報受信手段4 fによって受信されたコンテンツ鍵を復号するセッション鍵復号手段4 g、センタ秘密鍵によって、セッション鍵復号手段4 gにより復号されたコンテンツ鍵を暗号化するセンタ秘密鍵暗号化手段4 h、情報受信手段4 fによって受信されたコンテンツデータ、及びセンタ秘密鍵暗号化手段4 hによって暗号化されたコンテンツ鍵を格納するコンテンツデータ格納手段4 c、情報受信手段4 fによって受信されたコンテンツ情報を格納するコンテンツ情報格納手段4 b、利用者の個人情報を格納する個人情報格納手段4 a、付加情報提供者が提供するコンテンツ付加情報を格納するコンテンツ付加情報格納手段4 d、コンテンツ付加情報格納手段4 dから、各利用者に応じたコンテンツ付加情報を抽出するコンテンツ付加情報抽出手段4 m、コンテンツデータ格納手段4 cから、選択されたコンテンツデータ及びコンテンツ鍵を抽出するコンテンツ抽出手段4 i、コンテンツ抽出手段4 iによって抽出されたコンテンツ鍵をセンタ秘密鍵により復号するセンタ秘密鍵復号手段4 j、センタ秘密鍵復号手段4 jによって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段4 mによって抽出されたコンテンツ付加情報をセッション鍵によって暗号化するセッション鍵暗号化手段4 k、及び、コンテンツ抽出手段4 iにより抽出されたコンテンツデータ、及びセッション鍵暗号化手段4 kにより暗号化されたコンテンツ鍵及びコンテンツ付加情報を情報利用端末3に配信する情報配信手段4 lによって構成されている。

【0034】次に、本形態における情報保管配信システム1の動作について説明する。本システムは、利用者が事前に使用権を取得したコンテンツを情報保管配信装置4に送信・保管し、利用者がその保管したコンテンツを利用する際に、同時にコンテンツ付加情報の提供も受けられるというものである。以下、図1を用いて、情報保管配信システム1の概略動作について説明する。

【0035】本システムの利用にあたり、まず利用者は

17

個人情報の登録を行う。個人情報の登録は、郵送、或いはインターネットのWebページ等により行い、登録された個人情報は、情報保管配信装置4の個人情報格納手段4aに格納される。登録を行った利用者は、本システム提供者が発行する電子証明書を受け取り、受け取った電子証明書は、情報利用端末2、3が有する図示していないモジュールに格納される。

【0036】個人情報の登録を行った利用者は、次に、利用者が使用権を取得しているコンテンツの送信を行う。コンテンツの使用権の取得は、インターネットからのダウンロード等によって事前に行われており、そのように取得されたコンテンツデータ及びコンテンツ情報は情報利用端末2に格納されている。利用者は、このように情報利用端末2に格納されているコンテンツデータ及びコンテンツ情報を情報保管配信装置4に暗号化して送信し、情報保管配信装置4は、送信されたコンテンツデータをコンテンツデータ格納手段4cに、コンテンツ情報をコンテンツ情報格納手段4bにそれぞれ格納する。

【0037】また、付加情報提供者5は、各種のコンテンツ付加情報を情報保管配信装置4に送信し、コンテンツ付加情報を受け取った情報保管配信装置4は、受け取ったコンテンツ付加情報をコンテンツ付加情報格納手段4dに格納する。

【0038】利用者が情報保管配信装置4に送信したコンテンツを利用しようとする場合、まず利用者は、情報利用端末3を用いて情報保管配信装置4に接続し、情報保管配信装置4から送られるコンテンツデータ格納手段4cに格納されている自己のコンテンツデータのリストであるコンテンツリストを取得する。コンテンツリストを取得した利用者は、そのコンテンツリストを参照し、利用を希望するコンテンツを選択し、情報保管配信装置4からそのコンテンツデータの配信を受ける。この際、情報保管配信装置4は、利用者の個人情報及びコンテンツ情報等を参照し、その利用者に適したコンテンツ付加情報を抽出し、コンテンツデータとともに利用者に配信する。このようにすることにより、コンテンツデータの配信時に利用者に適した情報を自動的に提供することが可能となる。

【0039】次に、情報利用端末2、3と情報保管配信装置4での情報のやりとりについて説明する。まず、情報利用端末2から情報保管配信装置4へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置4への保管処理について説明する。図5及び図6は、これらの過程の動作手順を示した図である。

【0040】まず、情報利用端末2において送信GUIソフトウェアを起動し、情報利用端末2に格納されているコンテンツデータのリストを表示する。利用者は、表示されたリストを参照し、配信を希望するコンテンツデータ及びそのコンテンツ情報を選択する。選択されたコンテンツデータは、コンテンツ鍵により暗号化され、こ

18

の暗号化に用いられたコンテンツ鍵は、端末秘密鍵により暗号化される。

【0041】次に、情報利用端末2は情報保管配信装置4との認証処理を行い、セッション鍵の生成が行われる。セッション鍵の生成が終了すると、情報利用端末2は、そのセッション鍵を用い、選択されたコンテンツ情報、及び端末秘密鍵により暗号化されたコンテンツ鍵を暗号化する。そして、このように暗号化されたコンテンツ情報、コンテンツ鍵、及びコンテンツ鍵により暗号化されたコンテンツデータは、情報保管配信装置4に送信される。

【0042】情報利用端末2から送信されたコンテンツ情報及びコンテンツデータは、情報保管配信装置4に受信され、情報保管配信装置4のコンテンツデータ格納手段4cに格納される。一方、受信されたコンテンツ鍵は、セッション鍵によって復号され、次に、センタ秘密鍵により暗号化された後格納される。これらの情報の格納が終了すると、情報保管配信装置4は、情報の送信が完了した旨の信号を情報利用端末2に送る。

【0043】次に、コンテンツの配信動作について説明する。図7は、この過程の動作手順を示した図である。利用者が情報保管配信装置4に格納したコンテンツの配信を希望する場合、利用者は、まず、情報保管配信装置4との認証処理を行い、セッション鍵を生成する。セッション鍵が生成されると、情報保管配信装置4は、格納しているコンテンツのリストであるコンテンツリストを作成する。作成されたコンテンツリストは、セッション鍵によって暗号化され、暗号化されたコンテンツリストは情報利用端末3に送信される。

【0044】このように送信されたコンテンツリストは、情報利用端末3によって受信され、セッション鍵によって復号される。利用者は、復号されたコンテンツリストを参照して配信を希望するコンテンツの選択を行い、配送を希望するコンテンツの指定を行う。

【0045】コンテンツの指定は、情報保管配信装置4に伝えられ、情報保管配信装置4は、指定されたコンテンツデータ及びそのコンテンツ鍵をコンテンツデータ格納手段4cから抽出し、それに加え、利用者に適したコンテンツ付加情報をコンテンツ付加情報格納手段4dから抽出する。

【0046】このように抽出されたコンテンツ鍵、及びコンテンツ付加情報は、セッション鍵で暗号化され、コンテンツ鍵で暗号化されているコンテンツデータとともに情報利用端末3に配信される。情報利用端末3に配信されたコンテンツ鍵、コンテンツ付加情報及びコンテンツデータは、情報利用端末3によって受信され、これらを受信した情報利用端末3は、情報保管配信装置4に、配信が完了した旨の信号を送信する。

【0047】情報利用端末3によって配信されたコンテンツ鍵及びコンテンツ付加情報はセッション鍵で復号さ

19

れ、さらにコンテンツ鍵は端末秘密鍵で復号される。そして、情報利用端末3は、復号されたコンテンツ鍵を用い、コンテンツデータを復号し、復号したコンテンツデータ及びコンテンツ付加情報を格納する。

【0048】次に、図2から図4を用い、情報保管配信システム1の詳細動作について説明する。まず、情報利用端末2から情報保管配信装置4へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置4への保管処理について説明する。なお、以下の説明では、既に利用者の個人情報の登録は終了し、その個人情報は情報保管配信装置4の個人情報格納手段4aに格納されており、また、情報利用端末2のコンテンツデータ格納手段2aには利用者が使用権を取得したコンテンツデータが、コンテンツ情報格納手段2bにはそのコンテンツ情報がそれぞれ格納されているものとする。

【0049】まず、利用者は情報利用端末2が有するGUIソフトウェアを起動し、コンテンツデータ格納手段2aに格納されているコンテンツデータのリストを表示する。利用者は、表示されたリストを参照し、送信コンテンツ選択手段2cを用いて、配信を希望するコンテンツを指定する。送信コンテンツ選択手段2cは、利用者からの指定に従い、情報保管配信装置4に送信するコンテンツデータ及びそのコンテンツ情報をコンテンツデータ格納手段2a及びコンテンツ情報格納手段2bから抽出する。抽出されたコンテンツデータは、コンテンツ鍵暗号化手段2dにおいてコンテンツ鍵により暗号化され、この暗号化に用いられたコンテンツ鍵は、端末秘密鍵暗号化手段2eにおいて端末秘密鍵により暗号化される。

【0050】次に、認証手段2fにおいて、登録により取得した電子証明書を用い、情報保管配信装置4の認証手段4eとの認証処理を行う。この認証処理は、後述するAKE Protocol等を利用して行い、この認証処理の後、セッション鍵の生成が行われる。

【0051】セッション鍵の生成が終了すると、セッション鍵暗号化手段2hは、そのセッション鍵を用い、送信コンテンツ選択手段2cによって抽出されたコンテンツ情報、及び端末秘密鍵暗号化手段2eにおいて暗号化されたコンテンツ鍵を暗号化する。そして、セッション鍵暗号化手段2hにおいて暗号化されたコンテンツ情報、コンテンツ鍵、及びコンテンツ鍵暗号化手段2dにおいて暗号化されたコンテンツデータは、情報送信手段2iにより情報保管配信装置4に送信される。

【0052】情報利用端末2から送信されたコンテンツ情報、コンテンツ鍵及びコンテンツデータは、情報受信手段4fによって受信され、受信されたコンテンツ情報はコンテンツ情報格納手段4bに、コンテンツデータはコンテンツデータ格納手段4cにそれぞれ格納される。一方、受信されたコンテンツ鍵は、セッション鍵復号手段4gにおいてセッション鍵を用いて復号され、次に、

20

センタ秘密鍵暗号化手段4hにおいてセンタ秘密鍵により暗号化された後、コンテンツデータ格納手段4cに格納される。これにより、情報保管配信装置4に格納されたコンテンツを利用者等が不正に引き出すことを防止することができる。

【0053】なお、情報利用端末2は、GUIソフトウェアを用い、配信されるコンテンツの種類、順番等をエディットしたパッケージ情報を設定することが可能であり、コンテンツの送信時にこのパッケージ情報を送信することもできる。このように、送信されたパッケージ情報は、情報保管配信装置4のコンテンツ情報格納手段4bに格納される。

【0054】次に、付加情報提供者5によるコンテンツ付加情報の登録について説明する。付加情報提供者5は、情報保管配信システム1へのコンテンツ付加情報の提供にあたり、まず決済方法、契約条件等の登録を行う。登録は、郵送、或いはインターネットのWebページ等を用いて行われ、登録を行った付加情報提供者5は、情報保管配信装置4のWebサイトにアクセスするためのユーザID、パスワード等を取得する。

【0055】登録を終了した付加情報提供者5がコンテンツ付加情報の提供を希望する場合、付加情報提供者5は、取得したユーザID及びパスワードを用いて情報保管配信装置4のWebサイトにアクセスし、コンテンツ付加情報の送信を行う。このように送信されたコンテンツ付加情報は、情報保管配信装置4のコンテンツ付加情報格納手段4dに格納される。情報格納手段4dに格納されたコンテンツ付加情報は、付加情報提供者5の希望に応じて随時更新、変更され、情報格納手段4dには、常に最新の情報が保持される。

【0056】次に、コンテンツの配信動作について説明する。利用者が情報保管配信装置4に格納したコンテンツの配信を希望する場合、利用者は、電子証明書を用い、情報利用端末3の認証手段3aによって、情報保管配信装置4の認証手段4eとの認証処理を行う。この認証処理は、後述するAKE Protocol等を利用して行い、この認証処理の後、セッション鍵の生成が行われる。

【0057】セッション鍵が生成されると、情報保管配信装置4のコンテンツリスト作成手段4nは、コンテンツ情報格納手段4bに格納されたコンテンツ情報を用い、格納しているコンテンツのリストであるコンテンツリストを作成する。作成されたコンテンツリストは、コンテンツリスト暗号化手段4oによって暗号化され、暗号化されたコンテンツリストはコンテンツリスト送信手段4pによって情報利用端末3に送信される。なお、上述したパッケージ情報が作成されている場合には、コンテンツリストとともに、このパッケージ情報も送信されることとしてもよい。

【0058】このように送信されたコンテンツリスト等

21

は、情報利用端末3のコンテンツリスト受信手段3bによって受信され、受信されたコンテンツリスト等は、コンテンツリスト復号手段3cによって復号される。利用者は、復号されたコンテンツリストを参照して配信を希望するコンテンツの選択を行い、配信コンテンツ選択手段3dを用いて、配送を希望するコンテンツの指定を行う。配信コンテンツ選択手段3dによるコンテンツの指定は、情報保管配信装置4のコンテンツ抽出手段4iに伝えられ、コンテンツ抽出手段4iは、コンテンツデータ格納手段4cから指定されたコンテンツデータ及びそのコンテンツ鍵を抽出し、抽出されたコンテンツ鍵は、センタ秘密鍵復号手段4jによって復号される。

【0059】一方、コンテンツ付加情報抽出手段4mは、個人情報格納手段4a及びコンテンツ情報格納手段4bを元に、利用者に適したコンテンツ付加情報をコンテンツ付加情報格納手段4dから抽出する。

【0060】このようにセンタ秘密鍵復号手段4jによって復号されたコンテンツ鍵、及びコンテンツ付加情報抽出手段4mによって抽出されたコンテンツ付加情報は、セッション鍵暗号化手段4kにおいてセッション鍵で暗号化される。このようにセッション鍵で暗号化されたコンテンツ鍵及びコンテンツ付加情報は、コンテンツ鍵で暗号化されているコンテンツデータとともに、情報配信手段4lによって情報利用端末3に配信される。

【0061】配信されたコンテンツ鍵、コンテンツ付加情報及びコンテンツデータは、情報利用端末3の情報受信手段3eによって受信され、これらを受信した情報利用端末3は、情報保管配信装置4に、配信が完了した旨のメッセージを送信する。情報保管配信装置4は、このメッセージを受け取ると、配信したコンテンツの情報等を使用履歴として残し、その使用履歴を課金処理、マーケティング情報等に利用する。

【0062】一方、情報受信手段3eによって配信されたコンテンツ鍵及びコンテンツ付加情報は、セッション鍵復号手段3fにおいて、セッション鍵で復号され、また、セッション鍵復号手段3fによって復号されたコンテンツ鍵は、さらに端末秘密鍵復号手段3gにおいて、端末秘密鍵で復号される。そして、コンテンツ鍵復号手段3hは、端末秘密鍵復号手段3gで復号されたコンテンツ鍵を用い、コンテンツデータを復号する。

【0063】以上のように復号されたコンテンツ付加情報、コンテンツ鍵及びコンテンツデータは、図示していない情報利用端末3の記録装置に格納され、これらのデータによってコンテンツ及びコンテンツ付加情報の表示等が行われる。

【0064】図8は、AKE Protocolを用いた認証処理の様子を示した図である。この図において、Ecenterとは、情報保管配信装置4側のセンタ公開鍵e centerを用いた暗号化関数であり、Euserとは、電子証明書に含まれる端末公開鍵e userを用いた暗号化関数で

22

あり、Dcenterとは、情報保管配信装置4側のセンタ秘密鍵d centerを用いた復号化関数であり、Duserとは、端末側秘密鍵d userを用いた復号化関数である。情報利用端末2は、端末側秘密鍵d user及び端末公開鍵e userを有しており、登録時にセンタ公開鍵e centerを取得する。一方、情報保管配信装置4は、センタ公開鍵e center、センタ秘密鍵d center及び端末公開鍵e userを有している。

【0065】まず、情報利用端末2は、乱数r1を生成し、e centerを用いてr1を暗号化し($C1 = E_{center}(r1)$)を生成する)、C1を情報保管配信装置4に送る。情報保管配信装置4は、d centerを用いてC1を復号する($t1 = D_{center}(C1)$)を生成する)。また、情報保管配信装置4は、乱数r2を生成し、e userを用いてr2を暗号化し($C2 = E_{user}(r2)$)を生成する)、t1とC2を情報利用端末2に送る。

【0066】情報利用端末2は、t1=r1であるか否かを判断し、t1=r1である場合、d userを用いてC2を復号し($t2 = D_{user}(C2)$)を生成する)、t2を情報保管配信装置4に送る。

【0067】情報保管配信装置4では、t2=r2であるか否かを判断し、t2=r2である場合、セッション鍵Kを生成し、e userを用いてKを暗号化する($S = E_{user}(K)$)を生成する)。Sは情報利用端末2に送られる。

【0068】情報利用端末2は、d userを用いてSを復号する($K = D_{user}(S)$)を生成する)。その後、情報利用端末2と情報保管配信装置4との情報のやりとりには、このセッション鍵が使用される。

【0069】なお、以上の説明では、情報利用端末2と情報保管配信装置4との認証処理について説明したが、情報利用端末3と情報保管配信装置4との認証処理も同様な手順によって行われる。

【0070】このように、本形態では、利用者が使用権を取得したコンテンツを、情報利用端末2を用いて情報保管配信装置4に送信し、情報保管配信装置4は、そのコンテンツを保管し、利用者が情報保管配信装置4に格納されたコンテンツの利用を希望する場合、利用者は情報利用端末3を用いて情報保管配信装置4に格納されたコンテンツの配信を要求し、情報保管配信装置4は、要求されたコンテンツを情報利用端末3に配信することとしたため、利用者は、利用者が所持する記録装置の記憶容量に制限されることなく、コンテンツを保有することが可能となる。

【0071】また、コンテンツは情報保管配信装置4に格納され、コンテンツの管理は、情報保管配信装置4によって行われることとしたため、管理上の利便性が高まり、再生時におけるコンテンツの選択が容易になる。

【0072】さらに、コンテンツは情報保管配信装置4に格納され、利用者は、情報利用端末3を用い、情報保

23

管配信装置 4 から配信されたコンテンツを利用することとしたため、記録媒体を所持していない状況下であってもコンテンツの再生が可能となる。

【0073】また、コンテンツの再生のために記録媒体を用いないため、情報利用端末 3 は、記録媒体の収納スペース、及び記録媒体再生のための駆動部を設ける必要がなくなり、情報利用端末 3 の小型化を図ることが可能となる。

【0074】さらに、情報保管配信装置 4 は、情報利用端末 3 にコンテンツの配信を行う際、利用者の適した個人向け情報であるコンテンツ付加情報を送信することとしたため、各利用者は、自己が必要とする情報を自動的に入手することが可能となる。

【0075】なお、上記の処理機能は、コンピュータによって実現することができる。その場合、情報利用端末 2、3 及び情報保管配信装置 4 が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておく。そして、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリ等がある。市場に流通させる場合には、CD-ROM (Compact Disk Read Only Memory) やフロッピーディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。ここでコンピュータとは、特にパーソナルコンピュータには限定されず、少なくとも 1 つの処理装置を有し、プログラムによって制御されるコンピュータ一般を意味する。

【0076】また、本形態では、情報利用端末 2 と情報利用端末 3 を別々に構成することとしたが、情報利用端末 2 と情報利用端末 3 とを一体化する構成としてもよい。

【0077】

【発明の効果】以上説明したように本発明の情報利用端末では、使用権を取得したコンテンツを情報保管配信装置に送信することとしたため、使用権を取得したコンテンツを制限なく保有することができ、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、装置の小型化を図ることが可能となる。

【0078】また、本発明の情報利用端末では、情報保管配信装置に記録しておいた使用権を取得したコンテンツを選択し、情報保管配信装置から配信されたコンテンツを利用することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生

24

時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【0079】さらに、本発明の情報保管配信装置では、情報利用装置から送信されたコンテンツを保管し、利用者からの要求に応じて格納したコンテンツを抽出し、抽出したコンテンツをコンテンツ付加情報とともに情報利用端末に配信することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【0080】また、本発明の情報保管配信システムでは、情報利用端末によって、使用権を取得したコンテンツを情報保管配信装置に送信し、情報保管配信装置によって、情報利用装置から送信されたコンテンツを保管し、利用者からの要求に応じて格納したコンテンツを抽出し、抽出したコンテンツをコンテンツ付加情報とともに情報利用端末に配信し、情報利用端末によって、情報保管配信装置に記録しておいた使用権を取得したコンテンツを選択し、情報保管配信装置から配信されたコンテンツを利用することとしたため、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【0081】さらに本発明の記録媒体に格納されたプログラムをコンピュータ上で実行させることにより、使用権を取得したコンテンツを制限なく保有でき、管理上の利便性を高めて再生時におけるコンテンツの選択を容易にし、記録媒体を所持していない状況下におけるコンテンツの再生を可能とし、情報利用端末の小型化を図り、利用者に適した各種情報の提供を行うことが可能となる。

【図面の簡単な説明】

【図 1】情報保管配信システムの概略構成を示した構成図である。

【図 2】情報利用端末の構成を示した構成図である。

【図 3】情報利用端末の構成を示した構成図である。

【図 4】情報保管配信装置の構成を示した構成図である。

【図 5】情報利用端末から情報保管配信装置へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置への保管処理における動作手順を示した図である。

【図 6】情報利用端末から情報保管配信装置へのコンテンツの送信、及び送信されたコンテンツの情報保管配信装置への保管処理における動作手順を示した図である。

25

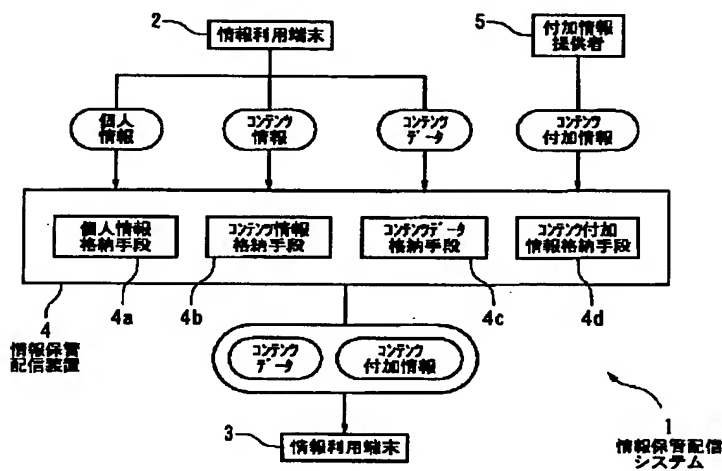
【図7】コンテンツの配信動作手順を示した図である。

【図8】AKE Protocolを用いた認証処理の様子を示した図である。

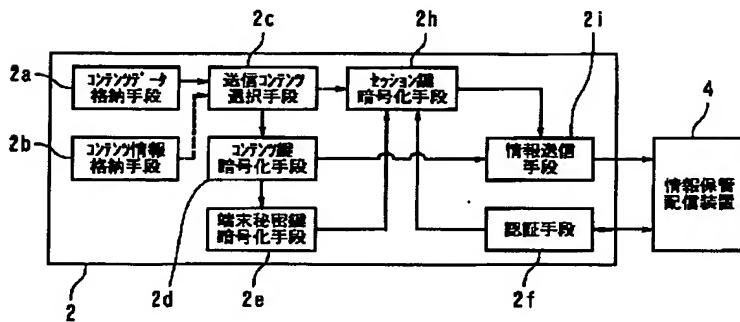
【符号の説明】

1…情報保管配信システム、2、3…情報利用端末、2 a…コンテンツデータ格納手段、2 b…コンテンツ情報格納手段、2 c…送信コンテンツ選択手段、2 d…コンテンツ鍵暗号化手段、2 e…端末秘密鍵暗号化手段、2 f、3 a、4 e…認証手段、2 h…セッション鍵暗号化手段、2 i…情報送信手段、3 b…コンテンツリスト受信手段、3 c…コンテンツリスト復号手段、3 d…配信コンテンツ選択手段、3 e…情報受信手段、3 f…セッション鍵復号手段、3 g…端末秘密鍵復号手段、3 h…コンテンツ鍵復号手段、4 a…個人情報格納手段、4 b…コンテンツ情報格納手段、4 c…コンテンツデータ格納手段、4 d…コンテンツ付加情報格納手段、4 f…情報受信手段、4 g…セッション鍵復号手段、4 h…センタ秘密鍵暗号化手段、4 i…コンテンツ抽出手段、4 j…センタ秘密鍵復号手段、4 k…セッション鍵暗号化手段、4 l…情報配信手段、4 m…コンテンツ付加情報抽出手段、4 n…コンテンツリスト作成手段、4 o…コンテンツリスト暗号化手段、4 p…コンテンツリスト送信手段

【図1】



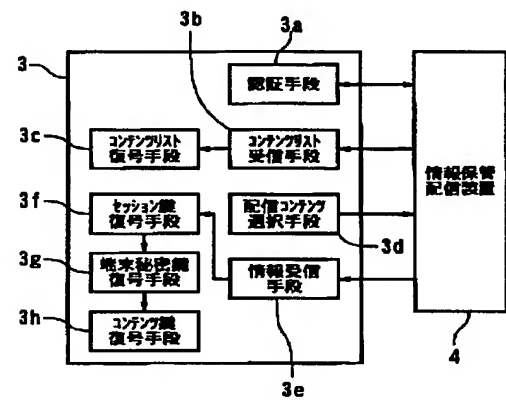
【図2】



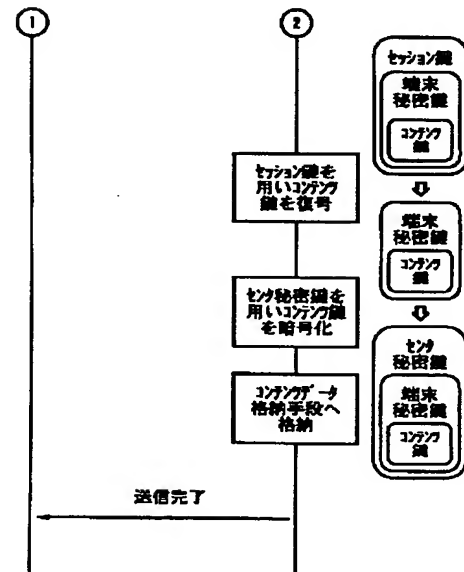
26

*セッション鍵復号手段、3 g…端末秘密鍵復号手段、3 h…コンテンツ鍵復号手段、4 a…個人情報格納手段、4 b…コンテンツ情報格納手段、4 c…コンテンツデータ格納手段、4 d…コンテンツ付加情報格納手段、4 f…情報受信手段、4 g…セッション鍵復号手段、4 h…センタ秘密鍵暗号化手段、4 i…コンテンツ抽出手段、4 j…センタ秘密鍵復号手段、4 k…セッション鍵暗号化手段、4 l…情報配信手段、4 m…コンテンツ付加情報抽出手段、4 n…コンテンツリスト作成手段、4 o…コンテンツリスト暗号化手段、4 p…コンテンツリスト送信手段

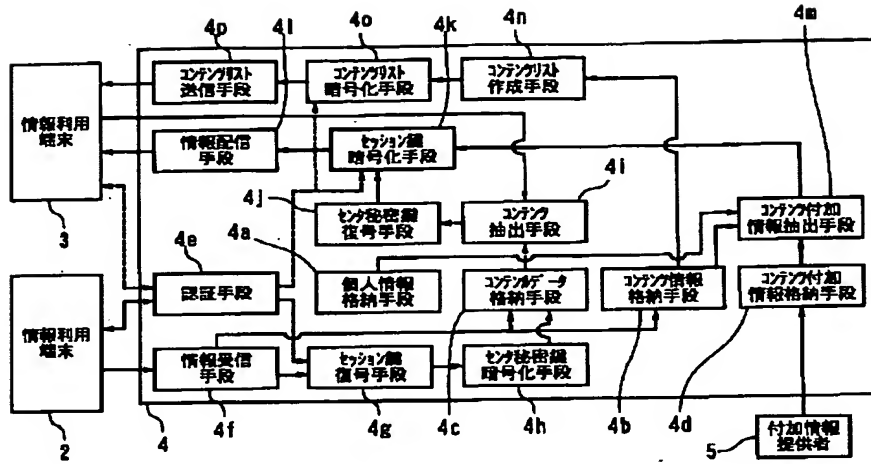
【図3】



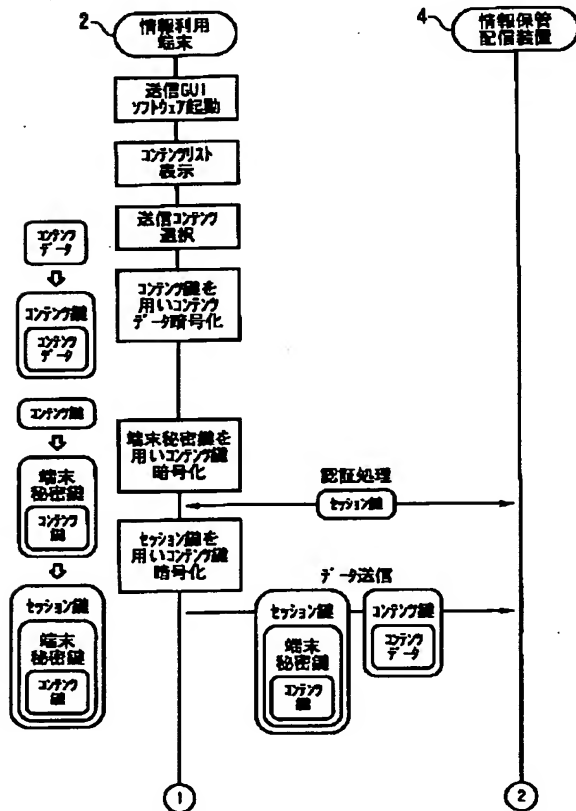
【図6】



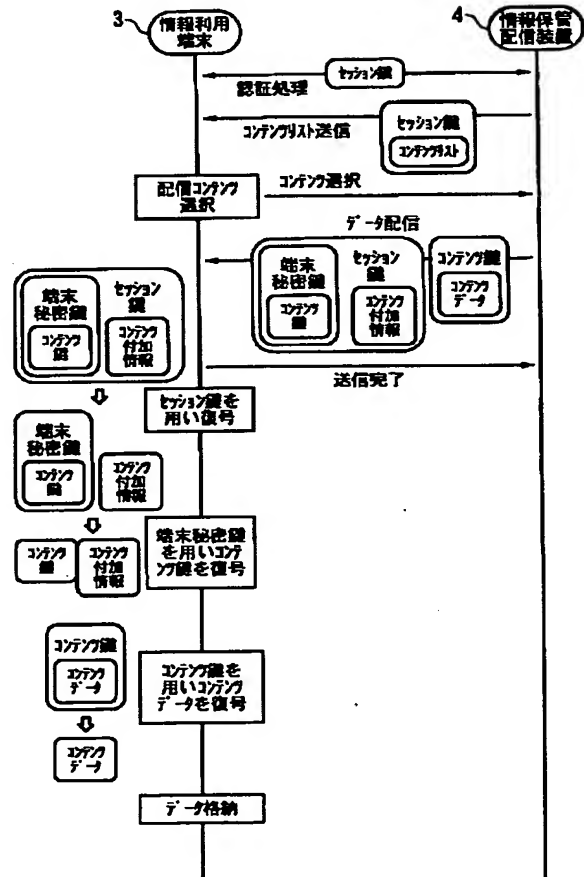
【図4】



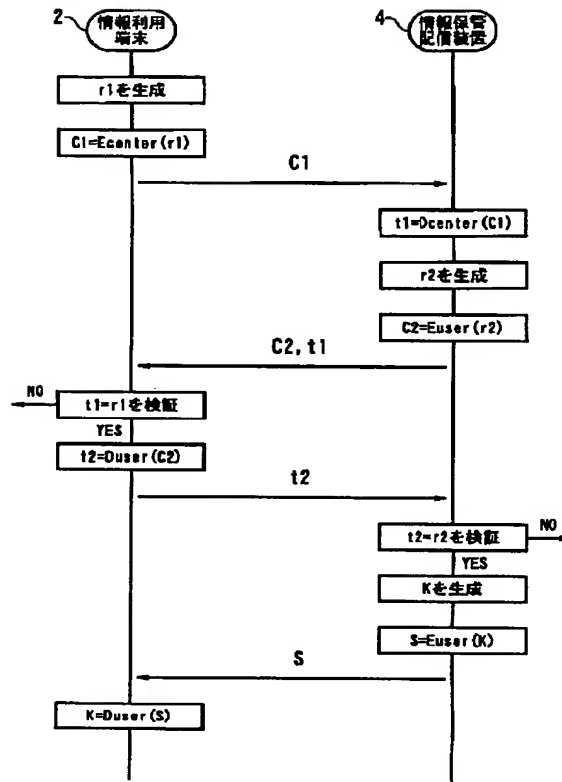
【図5】



【図7】



【図8】



フロントページの続き

(51) Int. Cl. 7

H 0 4 L 9/08
9/32

識別記号

F I

H 0 4 L 9/00

ターミナル (参考)

6 0 1 B 5 J 1 0 4
6 0 1 E
6 7 3 B

Fターム (参考) 5B017 AA07 BA07 CA16
 5B049 AA01 BB00 EE05 FF07 GG02
 GG10
 5B082 EA11 HA05
 5B085 AE29
 5B089 GA21 GB04 HA10 JA33 JB22
 KA11 KA13 KA17 KB04 KB13
 KC58 KH30 LB01 LB14
 5J104 AA01 AA07 AA16 EA04 EA07
 EA18 EA19 JA03 KA02 NA03
 NA27 PA07